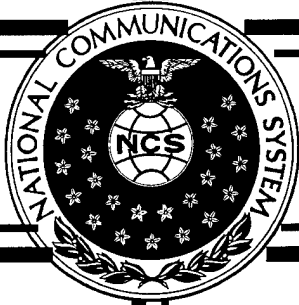


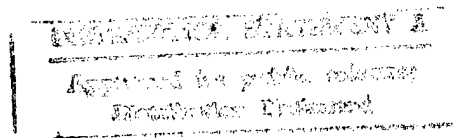
NCS TIB 95-1



NATIONAL COMMUNICATIONS SYSTEM

TECHNICAL INFORMATION BULLETIN 95-1

SECURITY AND FACSIMILE



FEBRUARY 1995

OFFICE OF THE MANAGER
NATIONAL COMMUNICATIONS SYSTEM
701 SOUTH COURT HOUSE ROAD
ARLINGTON, VA 22204-2198

19970117 051

95-4757

| REPORT DOCUMENTATION PAGE | | | Form Approved OMB No. 0704-0188 | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|-------------------------------------------------------|------------------------------------------------------------------------|--------------------------------------------------|
| Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503. | | | | |
| 1. AGENCY USE ONLY (Leave blank) | | 2. REPORT DATE February 1995 | | 3. REPORT TYPE AND DATES COVERED Final Report |
| 4. TITLE AND SUBTITLE Security and Facsimile | | | 5. FUNDING NUMBERS DCA100-91-C-0031 | |
| 6. AUTHOR(S) Stephen Perschau | | | | |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Delta Information Systems, Inc. Bldg 3, Suite 120 300 Welsh Road Horsham, PA 19044-2273 | | | 8. PERFORMING ORGANIZATION REPORT NUMBER | |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) National Communications System Office of Technology and Standards Division 701 South Court House Road Arlington, Virginia 22204-2198 | | | 10. SPONSORING/MONITORING AGENCY REPORT NUMBER NCS TIB #95-1 | |
| 11. SUPPLEMENTARY NOTES This report supersedes NCS TIB #93-16. | | | | |
| 12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited. | | | 12b. DISTRIBUTION CODE | |
| 13. ABSTRACT (Maximum 200 words) In addition to the secure transmission of the facsimile data, a second area of concern is the authentication of the sender and receiver, i.e., the sender is the true originator of the document and the receiver is the intended recipient of the document. The prior year report addressed the use of cryptosystems, both single/secret key and public key, in providing the secure data transmission and also authentication protocols within Group 3 and Group 4 facsimile. This report provides background information and the cryptosystems currently in use, discusses in detail contributions submitted by France Telecom to Study Group 8 regarding facsimile security, discusses in detail contributions submitted by the United Kingdom to Study Group 8 regarding facsimile security, discusses in detail existing Study Group 15 Recommendations which detail confidentiality/security for Audiovisual Services, and summarizes the report and reviews the current ongoing activities with regard to secure facsimile transmissions. | | | | |
| 14. SUBJECT TERMS Cryptosystem Keys Systems Secure Facsimile Group 3 Facsimile | | | 15. NUMBER OF PAGES 50 | |
| | | | 16. PRICE CODE | |
| 17. SECURITY CLASSIFICATION OF REPORT UNCLASS | 18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASS | 19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASS | 20. LIMITATION OF ABSTRACT UNLIMITED | |

GENERAL INSTRUCTIONS FOR COMPLETING SF 298

The Report Documentation Page (RDP) is used in announcing and cataloging reports. It is important that this information be consistent with the rest of the report, particularly the cover and title page. Instructions for filling in each block of the form follow. It is important to *stay within the lines* to meet *optical scanning requirements*.

Block 1. Agency Use Only (Leave blank).

Block 2. Report Date. Full publication date including day, month, and year, if available (e.g. 1 Jan 88). Must cite at least the year.

Block 3. Type of Report and Dates Covered. State whether report is interim, final, etc. If applicable, enter inclusive report dates (e.g. 10 Jun 87 - 30 Jun 88).

Block 4. Title and Subtitle. A title is taken from the part of the report that provides the most meaningful and complete information. When a report is prepared in more than one volume, repeat the primary title, add volume number, and include subtitle for the specific volume. On classified documents enter the title classification in parentheses.

Block 5. Funding Numbers. To include contract and grant numbers; may include program element number(s), project number(s), task number(s), and work unit number(s). Use the following labels:

| | |
|-----------------------------|-------------------------------------|
| C - Contract | PR - Project |
| G - Grant | TA - Task |
| PE - Program Element | WU - Work Unit Accession No. |

Block 6. Author(s). Name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. If editor or compiler, this should follow the name(s).

Block 7. Performing Organization Name(s) and Address(es). Self-explanatory.

Block 8. Performing Organization Report Number. Enter the unique alphanumeric report number(s) assigned by the organization performing the report.

Block 9. Sponsoring/Monitoring Agency Name(s) and Address(es). Self-explanatory.

Block 10. Sponsoring/Monitoring Agency Report Number. (If known)

Block 11. Supplementary Notes. Enter information not included elsewhere such as: Prepared in cooperation with...; Trans. of...; To be published in.... When a report is revised, include a statement whether the new report supersedes or supplements the older report.

Block 12a. Distribution/Availability Statement. Denotes public availability or limitations. Cite any availability to the public. Enter additional limitations or special markings in all capitals (e.g. NOFORN, REL, ITAR).

DOD - See DoDD 5230.24, "Distribution Statements on Technical Documents."

DOE - See authorities.

NASA - See Handbook NHB 2200.2.

NTIS - Leave blank.

Block 12b. Distribution Code.

DOD - Leave blank.

DOE - Enter DOE distribution categories from the Standard Distribution for Unclassified Scientific and Technical Reports.

NASA - Leave blank.

NTIS - Leave blank.

Block 13. Abstract. Include a brief (*Maximum 200 words*) factual summary of the most significant information contained in the report.

Block 14. Subject Terms. Keywords or phrases identifying major subjects in the report.

Block 15. Number of Pages. Enter the total number of pages.

Block 16. Price Code. Enter appropriate price code (*NTIS only*).

Blocks 17. - 19. Security Classifications. Self-explanatory. Enter U.S. Security Classification in accordance with U.S. Security Regulations (i.e., UNCLASSIFIED). If form contains classified information, stamp classification on the top and bottom of the page.

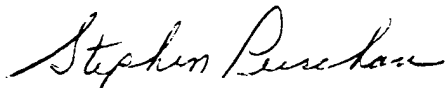
Block 20. Limitation of Abstract. This block must be completed to assign a limitation to the abstract. Enter either UL (unlimited) or SAR (same as report). An entry in this block is necessary if the abstract is to be limited. If blank, the abstract is assumed to be unlimited.

NCS TECHNICAL INFORMATION BULLETIN 95-1

SECURITY AND FACSIMILE

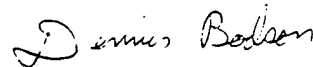
FEBRUARY 1995

PROJECT OFFICER



STEPHEN PERSCHAU
Computer Scientist
Office of Technology
and Standards

APPROVED FOR PUBLICATION:



DENNIS BODSON
Assistant Manager
Office of Technology
and Standards

FOREWORD

Among the responsibilities assigned to the Office of the Manager, National Communications System, is the management of the Federal Telecommunication Standards Program. Under this program, the NCS, with the assistance of the Federal Telecommunication Standards Committee identifies, develops, and coordinates proposed Federal Standards which either contribute to the interoperability of functionally similar Federal telecommunication systems or to the achievement of a compatible and efficient interface between computer and telecommunication systems. In developing and coordinating these standards, a considerable amount of effort is expended in initiating and pursuing joint standards development efforts with appropriate technical committees of the International Organization for Standardization, and the International Telegraph and Telephone Consultative Committee of the International Telecommunication Union. This Technical Information Bulletin presents an overview of an effort which is contributing to the development of compatible Federal, national, and international standards in the area of facsimile. It has been prepared to inform interested Federal activities of the progress of these efforts. Any comments, inputs or statements of requirements which could assist in the advancement of this work are welcome and should be addressed to:

Office of the Manager
National Communications System
Attn: NT
701 S. Court House Road
Arlington, VA 22204-2198

TASK 2
TECHNICAL WORK IN THE AREA OF FACSIMILE

SUBTASK 2
ENHANCEMENTS TO FACSIMILE

SECURITY AND FACSIMILE

FINAL REPORT
CONTRACT DCA100-91-C-0031
OPTION YEAR 3

Submitted to:
NATIONAL COMMUNICATIONS SYSTEM
ARLINGTON, VA

February, 1995

DELTA INFORMATION SYSTEMS, INC.
300 Welsh Road, Bldg. 3, Ste. 120
Horsham, PA 19044-2273
TEL: (215) 657-5270 **FAX: (215) 657-5273**

TABLE OF CONTENTS

| | |
|-----------------------------------------------------------------------------------------------------------------------------------|-------|
| 1.0 INTRODUCTION | 1 - 1 |
| 1.1 Report Organization | 1 - 1 |
| 2.0 SECURITY OVERVIEW | 2 - 1 |
| 2.1 Definitions | 2 - 5 |
| 3.0 FRANCE TELECOM CONTRIBUTIONS TO STUDY GROUP 8 | 3 - 1 |
| 3.1 Contribution 30 to Study Group 8 | 3 - 1 |
| 3.2 Delayed Contribution 107 to Study Group 8 | 3 - 5 |
| 3.3 Delayed Contribution 148 to Study Group 8 | 3 - 6 |
| 4.0 UNITED KINGDOM CONTRIBUTIONS TO STUDY GROUP 8 | 4 - 1 |
| 4.1 Contribution 59 to Study Group 8 | 4 - 1 |
| 4.2 Contribution 60 to Study Group 8 | 4 - 2 |
| 4.3 Contribution 61 to Study Group 8 | 4 - 5 |
| 4.4 Delayed Contributions D152 and D153 to Study Group 8 | 4 - 7 |
| 5.0 CONFIDENTIALITY, KEY MANAGEMENT AND AUTHENTICATION SYSTEM FOR AUDIOVISUAL SERVICES - STUDY GROUP 15 CONTRIBUTIONS | 5 - 1 |
| 5.1 Confidentiality System for Audiovisual Services - H.233 | 5 - 1 |
| 5.2 Encryption Key Management and Authentication For Audiovisual Services - H.234 | 5 - 2 |
| 6.0 SUMMARY AND RECOMMENDATIONS | 6 - 1 |
| 6.1 Summary | 6 - 1 |
| 6.2 Recommendations | 6 - 1 |

APPENDIX A - Delayed Contributions D152 and D153 to Study Group 8

1.0 INTRODUCTION

This document summarizes work performed by Delta Information Systems, Inc. (DIS) for the Office of Technology and Standards of the National Communications System, an organization of the U.S. Government. The effort was specified by Task 2, Subtask 2 of Contract number DCA100-91-C-0031 during Option Year 3. With the ever increasing widespread use of facsimile to transfer document information between individuals, businesses, and government facilities, it has become apparent that a secure mode of fax transmission needs to be available to the user. Most of the information sent via facsimile is of a non-sensitive nature (Sales Information, News Bulletins, etc) and does not need to be transferred securely because it is available from other sources. Other information such as competitive bids and sensitive internal corporate information being sent from one corporate office to another, could adversely affect the company if it is intercepted by a competitor.

In addition to the secure transmission of the facsimile data, a second area of concern is the authentication of the sender and receiver, i.e. the sender is the true originator of the document and the receiver is the intended recipient of the document. The prior year report⁽¹⁾ addressed the use of cryptosystems, both single/secret key and public key, in providing for secure data transmission and also authentication protocols within Group 3 and Group 4 facsimile. The current task will review activity during the past year with regards to secure facsimile.

1.1 Report Organization

This report has six sections:

- 1.0 Introduction
- 2.0 Overview
- 3.0 France Telecom Contributions to Study Group 8
- 4.0 United Kingdom Contributions to Study Group 8
- 5.0 Confidentiality, Key Management and Authentication system for Audiovisual Services - Study Group 15 Contributions
- 6.0 Summary and Recommendations

Section 1.0 provides background information and discusses this reports organization.

Section 2.0 provides an review of data transmission security and the cryptosystems currently in use.

Section 3.0 discusses in detail contributions submitted by France Telecom to Study Group 8 regarding facsimile security.

Section 4.0 discusses in detail contributions submitted by the United Kingdom to Study Group 8 regarding facsimile security.

Section 5.0 discusses in detail existing Study Group 15 Recommendations (e.g. H.233, H.KEY) which detail confidentiality/security for Audiovisual Services.

Section 6.0 summarizes the report and reviews the current ongoing activities with regard to secure facsimile transmissions.

2.0 SECURITY OVERVIEW

Most facsimile terminals today perform point to point communications between a sender and receiver. The first security issue with this type of data transmission is that it is possible for the facsimile data to be intercepted and displayed and/or changed without either party knowing that the information has been "stolen" and/or modified. Historically the solution to securing the data being transmitted is by using a cryptosystem to transform/encode the data being sent into scrambled/unintelligible data. The cryptosystem consists of encryption and decryption functions together with a set of keys that parameterize the functions. The encryption function scrambles the original data, also known as plaintext, into what appears as nonsense or ciphertext, while the decryption function restores the original data. (See Figure 2.1). The keys are not integral parts of the encryption and decryption functions, so the same functions can be used with many different keys. At least the decrypt key must be kept secret to prevent an unauthorized listener from decrypting intercepted ciphertext. The encrypt and decrypt functions may be made public because without the appropriate key the ciphertext can not be decrypted.

Currently there are two types of cryptosystems, single/secret-key systems and public-key systems. Prior to the late 1970's all generally known cryptosystems were single-key systems. A single-key cryptosystem is one in which the encryption and decryption keys are the same (or readily derived from each other). (See Figure 2.2) These cryptosystems are also referred to as secret-key or symmetric systems. Single-key cryptosystems provide authenticity because only the holders of the common single or secret key are able to create ciphertext that decrypts into meaningful plaintext. The main problem associated with single/secret-key cryptosystems is the secure exchange of the secret-key between the sender and receiver. If the key can not be exchanged securely then any subsequent transmissions using the key can be intercepted and decrypted. The generation, transmission and storage of keys is called key management and is common to all cryptosystems.

Public-key (or asymmetric) cryptosystems (See Figure 2.3) were invented in 1976 by Whitfield Diffie and Martin Hellman^[2] in order to solve the key management problem. In a public-key system, every person gets a pair of keys, one public, one private. Everyone publishes his public key and keeps his private key secret. The need for the sender and receiver to share a secret key is eliminated because all communications are encrypted by the sender using the receiver's public key. No private key is ever transmitted so its security is never in jeopardy. Anyone can send a confidential message using public information only. This message can only be decrypted with the secret key held by the intended recipient.

CRYPTOSYSTEM

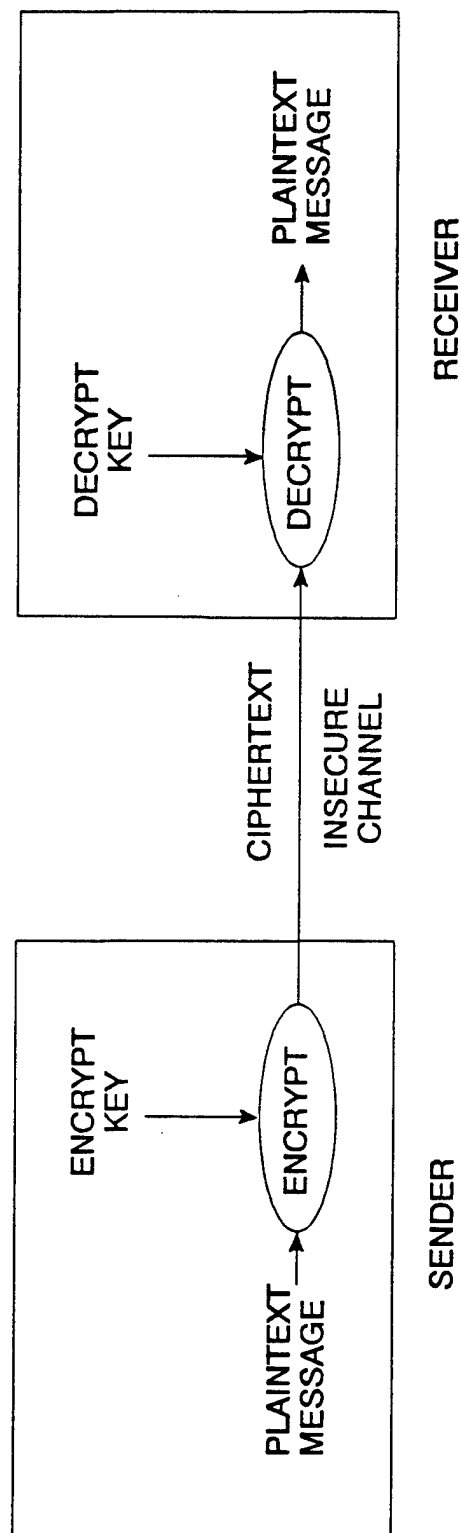


FIGURE 2.1

SINGLE-KEY CRYPTOSYSTEM

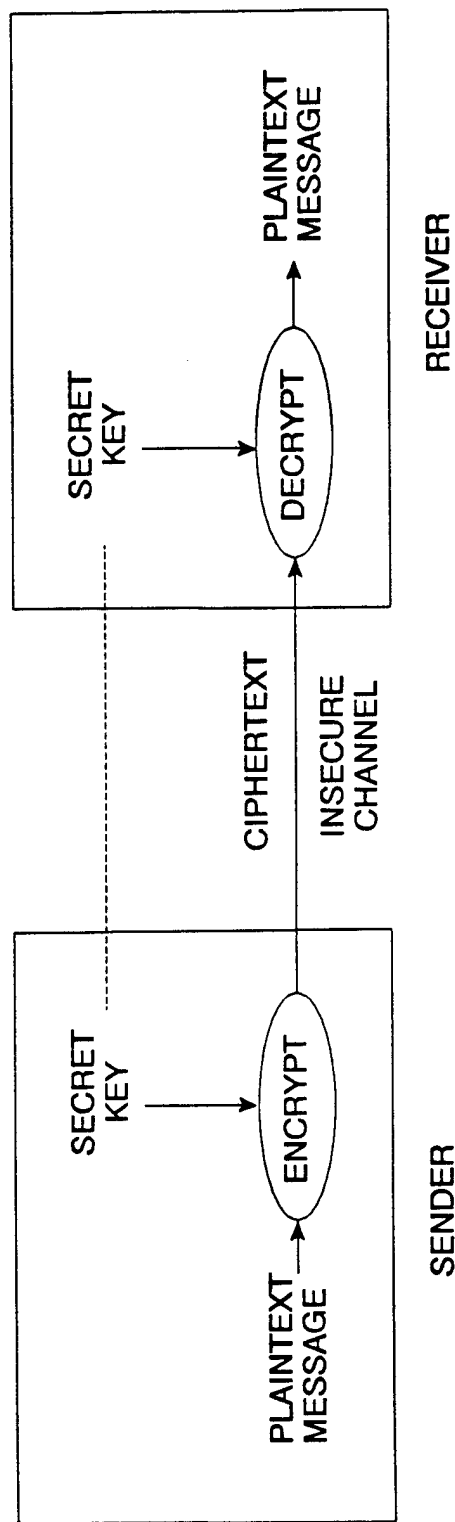


FIGURE 2.2

PUBLIC-KEY (TWO-KEY) CRYPTOSYSTEM

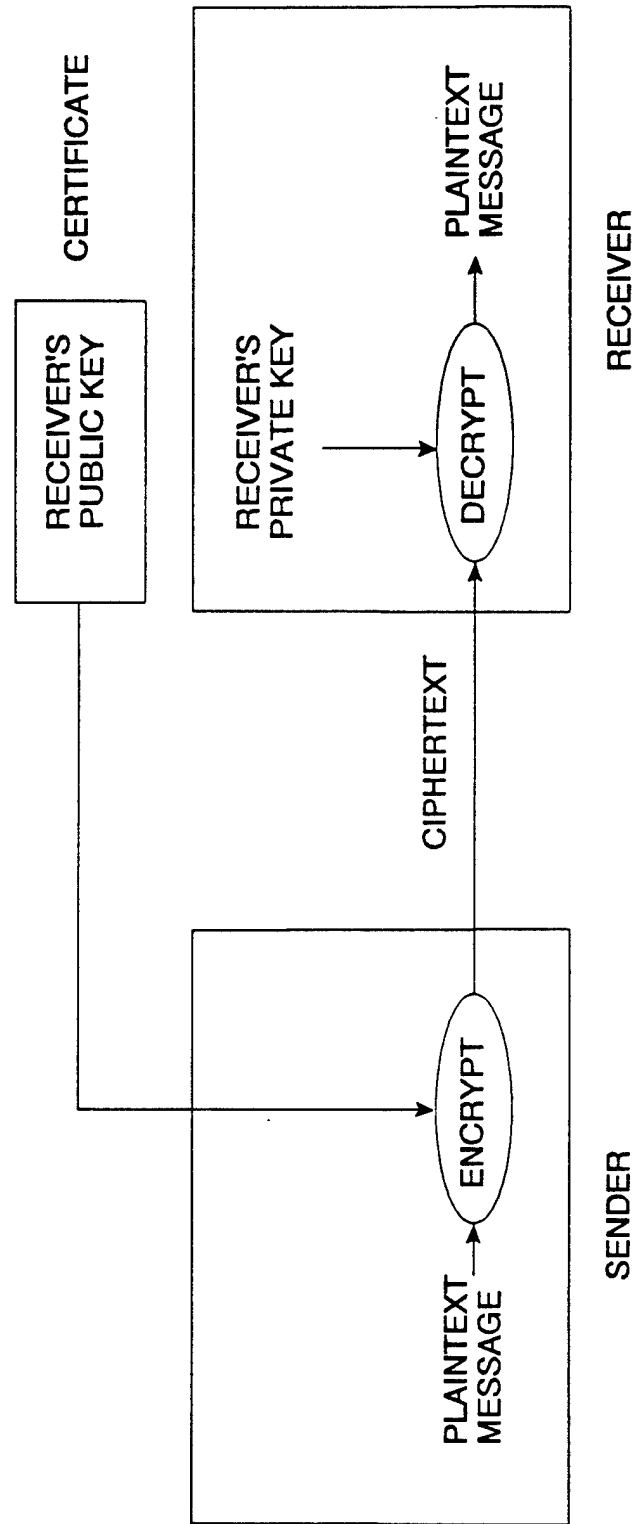


FIGURE 2.3

The second security issue is authentication, that is, the sender is the true originator of the document and the receiver is the intended recipient of the document. As noted above, authenticity is automatically provided by a single/secret key cryptosystem because only the holders of the secret key can encrypt/decrypt the message. In a public-key cryptosystem, authentication can be achieved through the use of digital signatures. A digital signature in digital communications plays the same role as a handwritten signature for printed documents. A digital signature is a block of data added to a digital message that binds the message to a particular individual or entity. A digital signature can be generated by the public-key cryptosystem itself (by using the private keys of the sender/receiver) or by a digital signature system. (See Figure 2.4) A digital signature system is similar to a public-key cryptosystem in that each user has a public and private key. The sender signs a message by sending a block of data (typically a "hash" of the message itself) encrypted with their private key, generating the digital signature. The receiver verifies the message by decrypting the signature block with the senders public key and comparing the contents with it's own "hash value of the message.

This report will review the ongoing work within Study Group 8 of the ITU as regards secure fax for both Group 3 and Group 4 facsimile. In addition, activities within the U.S effecting the use of cryptosystems within facsimile equipment will be discussed.

2.1 Definitions

Authentication - the process whereby the recipient of a message is assured that the identity of the sender and/or the integrity of the message.

Certificate - a digital document that binds a public key to an individual or other entity in a public-key system.

Certifying Authority - a trusted organization with whom a user registers their public key and then generates a certificate for that user.

DES - Data Encryption Standard as defined by the U.S. Government.

Digital Signature - a digital data block attached to a message that serves the same purpose as a handwritten signature on a paper document.

DSS - the Digital Signature Standard as proposed by NIST.

Hash Function - a mathematical function that takes a variable size input and returns a string of fixed size called the hash value.

Message-Digest Function - a one way hash function that takes a variable length message as input and generates a fixed length "message digest" as output. The resulting message digest can be viewed as a "digital fingerprint" of the original message.

PKCS - Public-Key Cryptography Standards - a set of standards for implementing public-key cryptography issued by RSA Data Security, Inc in cooperation with a computer industry consortium.

PUBLIC-KEY SIGNATURE SYSTEM

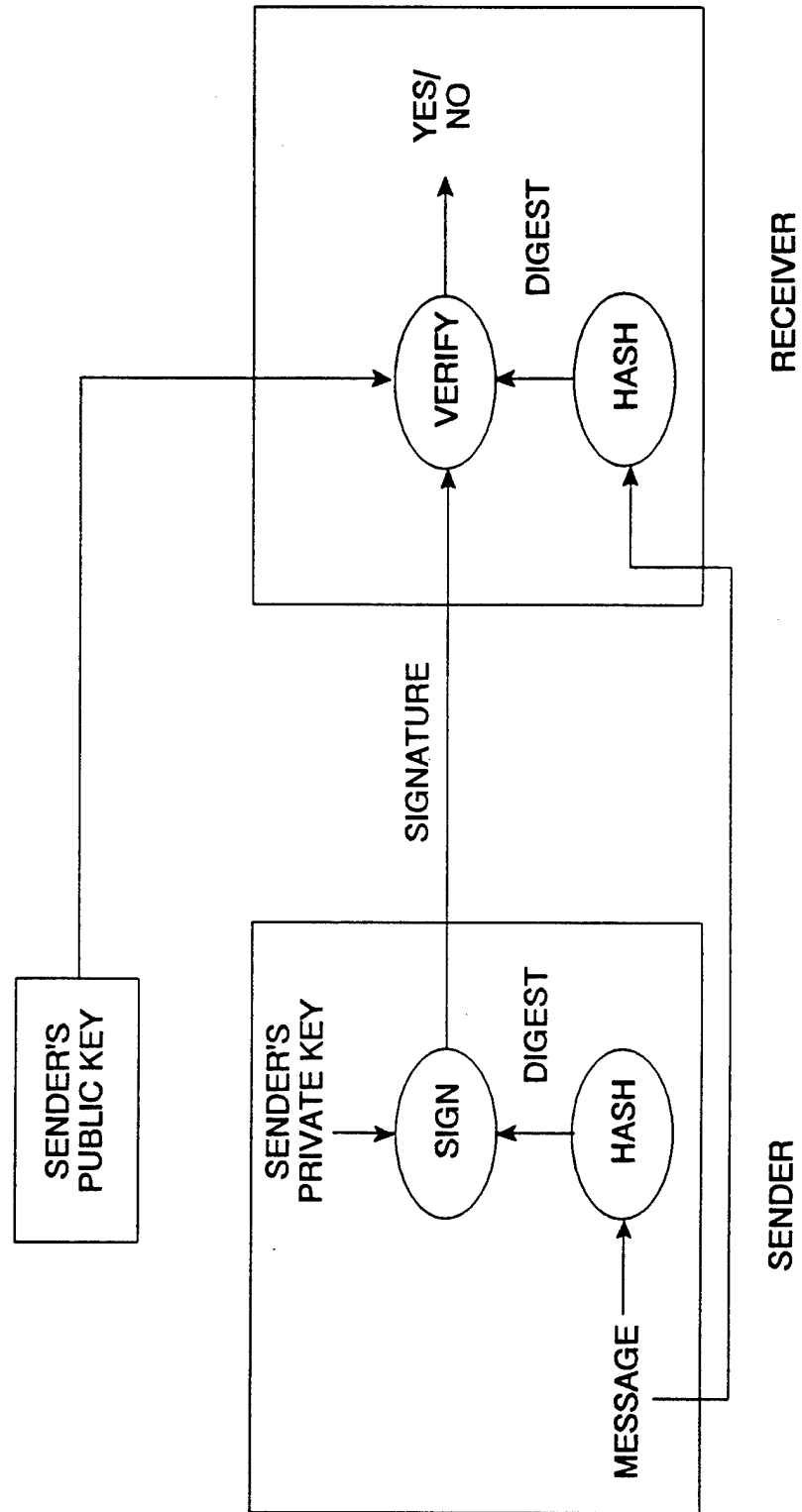


FIGURE 2.4

Public-Key Cryptosystem - a cryptosystem in which each user has a pair of keys, one public and one private. Also known as asymmetric systems.

RSA - a public-key encryption algorithm invented by Rivest, Shamir and Adelman of MIT.

SHS - Secure Hash Standard - a hash function used in the Digital Signature Standard.

Single-Key Cryptosystem - a cryptosystem in which two users share the same key which is used for both encryption and decryption. Also known as secret-key or symmetric systems.

3.0 FRANCE TELECOM CONTRIBUTIONS TO STUDY GROUP 8

In late 1993 and 1994, a series of contributions from France Telecom discussing security in facsimile were submitted to Study Group 8. The primary document, Com 8-30, describes the "security page" and other additional information required to support security services in Group 3 and Group 4 facsimile. This contribution also detailed its application to Group 3 facsimile and T.30. Subsequent delayed contributions, D107 and D148, describe the application of Com 8-30 to Group 4 facsimile and the authentication of the receiving side prior to the message transmission respectively. It should be noted that these documents do not discuss the use of specific key management facilities or encryption algorithms to be used but detail the information required to allow for authentication, data integrity, protection against replay, non-repudiation for origin and delivery, and data confidentiality.

3.1 Com 8-30

3.1.1 Security Services

This contribution describes the "security page" and the other additional information required in the protocol in order to offer security services. The security services provided are the following:

- Authentication
- Data Integrity
- Protection against replay
- Non-repudiation with proof of origin
- Non-repudiation with proof of delivery
- Data confidentiality

Authentication was divided into two levels:

- Identity of the user himself.
- Identity/telephone number of the facsimile terminal.

At the sending side, it was proposed that the authentication be based on the identity of the sending user. This identity would consist of the international telephone number of the sending facsimile plus a four digit sub-address unique to the user. At the receiving side, because the receiving user might not be present when the facsimile is received, authentication was based on the international telephone number of the receiving facsimile. Independent of whether the receiving user is present or not, the sender must indicate the identity of the recipient he wants to reach. This identity has the same format as the sender (international telephone number of the receiving facsimile plus the 4 digit sub-address).

3.1.2 Mechanisms For Security Services

It was proposed by Contribution 30 that digital signatures would provide almost all the security services required. Shown in Table 3.1 is a list of the data units to which digital signatures are applied and the security service this provides.

TABLE 3.1

| Digital signature applied to | Service fulfilled | |
|------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|--------------------------------------------------------|
| Identity of the sending user (this parameter should be sent by the emitting side) | Authentication of the emitting user | Non-repudiation with proof of origin |
| Identity of the recipient (this parameter should be sent by the emitting side) | Integrity of the address of the message | |
| Facsimile pages and numbers of the pages | Integrity of the facsimile data | |
| Date and time the sender has signed the message (these parameters should be sent by the emitting side) | Protection against replay and agreement upon date and time between the peers | |
| Acknowledgment by the receiving terminal of the origin and the content of the message received (this parameter should be sent by the receiving side) | Authentication of the receiving <u>terminal</u> | Non-repudiation with proof of delivery to the terminal |

Although no digital signature algorithm was specified in the contribution, it was thought that it should be unique to secured facsimile. It was further stated that if this is not achievable, the present approach is open to various algorithms and that the specific algorithm used could be negotiated within the protocol.

It was also proposed that if data confidentiality is required then an encipherment/encryption technique should be used. Only the facsimile page would be encrypted and the encryption algorithm should be based on the identity of the users (e.g. public key), thereby removing the need for the transmission of the encryption key. If the encryption key needs to be specific to the document (document being sent to many recipients) it is possible to encrypt the document with a "session key" which is encrypted by the identity-based encryption algorithm and sent during the communication.

3.1.3 Data Elements Needed for Security Services

In order to supply secure services for facsimile, additional data elements are required. The primary data element is a "security page" which is transmitted at the end of the facsimile document. In addition, some new data elements must be sent prior to the document transmission.

3.1.3.1 Security Page

The security page contains the following information:

- Identity of the recipient
- Identity of the sender
- Date and Time of the signature
- Number of pages in the document
- Digital Signature algorithm name/id
- Encryption algorithm name/id
- Session Key for current communication if required
- Digital Signature of the above information
- Digital Signature of each page (content and number)

Each field is identified by a field type octet so the fields may appear in any order within the data stream.

3.1.3.2 Additional Data Elements

In addition to the security page, other additional data elements are required. The following data elements must be sent prior to the transmission of the document. This information will be sent during phase B of T.30 protocol, the negotiation phase prior to the document transmission. It is assumed that any negotiation of security capabilities, e.g encryption enabled, will be done using the existing DIS/DCS/DTC mechanism.

Identity of the recipient intended by the sender
Identity of the receiving entity
Identity of the sender
Relationship between the user identity and the telephone number of the facsimile equipment (ID from a smart card etc.)
Date and time of signature
Mechanism against replay

In order to provide authentication of the receiving terminal along with non-repudiation with proof of delivery, the following information must be sent subsequent to the reception of the security page as an acknowledgement by the receiving terminal.

| | | |
|-------------------|---|--------------------------------------|
| Information Octet | - | 0 if facsimile successfully received |
| | - | Otherwise an error has occurred |

Digital Signature of the following:

Id of sender
Id of recipient
Information octet
Number of pages
Signatures of the received pages

3.1.4 Security Device Requirements

Com 8-30 discussed the use of two devices and their application to secure facsimile transmission. The devices consisted of a "security module" and a message store. The "security module" contains the sender identity and associated security elements (e.g. encryption keys). The message store is a method of storing messages at the receiving and/or sending side.

Two approaches to a "security module" were listed in the contribution. The first being a removable device (e.g. smart card) and the second being a device embedded in the fax terminal itself. The first approach, use of a smart card, is an inherently safe solution because all the security data elements are held by the user and the digital signature can be processed inside the security module. In addition, this solution also permits the use of the secured fax by multiple users via their smart card. The second approach has the disadvantage of requiring access control to the secured facsimile terminal.

A message store device is required to satisfy additional security services. If confidentiality is needed at the receiving side then the message store is necessary for each user of the facsimile terminal. If non-repudiation is needed then the secured document (with the digital signature) must be archived. For the sending terminal, the archived document along with the archived acknowledgement by the receiving terminal insures non-repudiation with proof of delivery. At the receiving terminal it insures non-repudiation with proof of origin.

3.1.5 Application to Group 3 Facsimile

In order to support a secure facsimile environment, the Group 3 facsimile terminal must have the following capabilities:

- Error Correction Mode (ECM)
- Coding and transmittal of the security page as the last page in the communication. All fields of the security page are coded in conformance with Recommendation T.4 Annex D using character mode. Each field corresponds to one line with fields being separated by "CR LF" in conformance with T.4. Since character mode specifies a maximum of 55 lines per page and the security page has six header fields, this limits the total number of pages in a secured facsimile to 49 pages.

- Ability to negotiate the security capabilities within the T.30 protocol.
- Ability for the sending terminal to send the additional data elements required to support the secure services.
- Ability for the receiving terminal to send the acknowledgement upon receipt of the secured facsimile.

3.2 Delayed Contribution 107 to Study Group 8

Subsequent to the introduction of COM 8-30 to Study Group 8 which detailed an approach to the implementation of secure facsimile and its application to Group 3 facsimile, Delayed Contribution 107 was introduced which details its application to Group 4 facsimile. Although this contribution restates all the principles of security defined in COM 8-30 which we detailed in the previous section, only their application to Group 4 facsimile will be discussed in this section.

3.2.1 Application to Group 4 Facsimile

The following details the additions/changes needed to the Group 4 protocol to support secure facsimile. The secure services implemented are identical to those discussed in Section 3.1 for Group 3 Facsimile.

3.2.1.1 Negotiation of Security Facilities

Negotiation of security facilities follows the same rules that apply for all optional characteristics of Group 4 facsimile. The facsimile terminals will indicate their security facilities during the establishment procedure using the D-INITIATE service. The security mode and the encryption option parameters will be added to the Document application profile within the Application capabilities transferred during the D-INITIATE service.

3.2.1.2 Transfer of Additional Data Elements Prior to Document

Within the Group 4 protocol the following data elements are sent by the sending terminal:

- Identity of the intended recipient
- Identity of the sender (user)
- Date and time of the digital signature

The receiving terminal returns the following data elements:

- Identity of the receiving entity
- Signature of the three elements sent by the sending entity

Two possible solutions for sending the data elements were discussed in D 107:

- Use the Document Transfer And Manipulation (DTAM) protocol elements with the D-CAPABILITY procedure
- Use the Open Document Architecture (ODA) facilities, during the transmission of the document, with the Document Profile

Since it is very important to verify the identity of the receiver before sending the document, using the DTAM protocol elements with the D-CAPABILITY procedure is the preferred method. The sending terminal will send the data elements listed above as part of the Application capabilities within the D-CAPABILITY Request. Correspondingly the receiving terminal will send the data element listed above as part of the Application capabilities within the D-CAPABILITY Response. This provides the sending terminal the opportunity to verify the identity of the receiving terminal prior to the sending of the document.

3.2.1.3 Initiation of the Security Mode

After completion of the negotiations, the sender can invoke the security mechanisms. The initiation of the security mechanisms is done by specifying the security mode and encryption option within the Document information attribute of the D-TRANSFER service.

3.2.1.4 Transfer of the Security Page

As in Group 3 facsimile, the security page is transmitted as the last page of the document. The coding of the security page is the same for Group 3 and Group 4. All fields of the security page are coded in conformance with Recommendation T.4 Annex D using character mode. Each field corresponds to one line with fields being separated by "CR LF" in conformance with T.4. As in Group 3, a secure facsimile is limited in length to 49 pages. (Ref Sec 3.1.5)

3.2.1.5 Acknowledgement by the Receiving Terminal

The acknowledgement consists of an information octet indicating the status of the transfer (successful or not) and the digital signature of the security page information. This acknowledgement is sent by the receiving terminal to the sending terminal as a one page document. The transfer of the acknowledgement is done within the D-CONTROL-GIVE procedure which permits the receiving terminal to send a document to the sending terminal.

3.3 Delayed Contribution 148 to Study Group 8

Submitted to Study Group 8 in Geneva in June 1994, this contribution was an enhancement to COM 8-30. In particular, it detailed the procedures for authentication of the receiving facsimile terminal prior to message transmission. Although the entire content of COM 8-30 was included in this contribution, the only other changes to the document were cosmetic in nature.

3.3.1 Security Services

This contribution added no new security services to Group 3 or Group 4 facsimile.

3.3.2 Mechanisms for Security Services

As in COM 8-30, digital signatures are the primary mechanisms used to provide security services. In order to provide for the authentication of the receiving terminal, Table 1 in COM 8-30 was updated to reflect the sending of the identity of the receiver by the receiving side. Shown in Table 3.2 below is the revised Table 1.

TABLE 3.2

| Digital signature applied to | Service fulfilled | |
|------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|--------------------------------------------------------|
| Identity of the sending user (this parameter should be sent by the emitting side) | Authentication of the emitting user | Non-repudiation with proof of origin |
| Identity of the recipient (this parameter should be sent by the emitting side) | Integrity of the address of the message | |
| Facsimile pages and numbers of the pages | Integrity of the facsimile data | |
| Date and time the sender has signed the message (these parameters should be sent by the emitting side) | Protection against replay and agreement upon date and time between the peers | |
| Identity of the receiving entity (this parameter should be sent by the receiving side) | Authentication of the receiving entity before the message is sent | |
| Acknowledgment by the receiving terminal of the origin and the content of the message received (this parameter should be sent by the receiving side) | | Non-repudiation with proof of delivery to the terminal |

3.3.3 Data Elements Needed for Security Services

Added to the list of data elements required to support the security service was the signature of the identity of the receiving terminal. It was specified that an information octet (indicating whether the signature is from the receiving terminal or the actual recipient) along with this signature be sent by the receiving terminal as octets appended to the Confirmation to Receive (CFR) response. The digital signature is applied to the following data elements:

- Information octet
- Identity of the receiving entity
- Identity of the sender
- Identity of the recipient intended by the sender

3.3.4 Application to Group 3 and Group 4 Facsimile

The application of the above additions to Group 3 Facsimile is also detailed in Contribution D148. Specifically it defines the structure of the CFR response and the additional octets added for the transmission of the receivers identity. Since the transmission of the receivers identity was already present within the Group 4 protocol as part of the D-CAPABILITY procedure, no change was required to Contribution D107.

4.0 UNITED KINGDOM CONTRIBUTIONS TO STUDY GROUP 8

During 1994, a series of contributions from the United Kingdom discussing security in facsimile were submitted to Study Group 8. Three Contributions, COM 8-59, COM 8-60 and COM 8-61 discuss "Security Requirements for Group 3 Facsimile", "Proposed Security System for Group 3 Facsimile", "Incorporation of Security Features into Recommendation T.30" respectively. The first of these three contributions, COM 8-59, reviews secure facsimile requirements and recommends the use of the Hawthorne Key Management (HKM) System. In addition, this contribution gives a brief description of the HKM system and the HFX40 encryption system. Contribution COM 8-60 provides a further description of the registration and automatic modes within the HKM system. COM 8-61 proposes a method of incorporating the features needed for HKM system within Recommendation T.30. Two delayed contributions to Study Group 8, D152 and D153, describe in detail the HKM key management system and HFX40 encryption system respectively. In contrast to the Contributions submitted by France Telecom, which did not address the specific algorithms to be used to achieve secure facsimile services, these contributions outline a specific approach to the exclusion of others. The following is a detailed review of each of the United Kingdom contributions.

4.1 COM 8-59

COM 8-59, "Security Requirements for Group 3 Facsimile", reviews the security requirements for Group 3 facsimile, details the shortcomings of the existing approaches and then proposes the use of the Hawthorne Key Management system along with its associated encryption algorithm, HFX40, to meet the security requirements for Group 3 facsimile. The following is a summary of COM 8-59.

4.1.1 Encryption and Key Management Systems

COM 8-59 begins with a review of the key management requirements for the following three encryption systems:

- Private Key Encryption Systems
- RSA Public Key encryption System
- Diffie-Hellman System

It details the deficiencies with each of the above systems. The private key encryption system's primary problem is the management of the extremely large number of keys to support a worldwide facsimile network. The RSA Public Key encryption system's primary problem is the generation of a unique set of large prime numbers for every facsimile terminal and the high cost of generating those prime numbers. The Diffie-Hellman system's primary problem is that while it provides security on line, it does not guarantee authentication of the sender. An additional problem is that it requires prime numbers greater than 120 decimal digits.

4.1.2 Hawthorne Key Management System

The contribution then proposes the use of the Hawthorne Key Management (HKM) System as an alternative to the above approaches. The following advantages of the HKM system are listed:

- Instead of large prime numbers the HKM system uses random length strings put in the facsimile terminal by the manufacturer.
- The operation of decrypting a message authenticates both the sender and the receiver.
- A registration procedure is used only once to exchange the information required to secure all future transmissions.
- The key management encryption algorithm can be used as the data encryption algorithm (HFX40) reducing the implementation complexity.

COM 8-59 also gives a brief description of the encryption algorithm (HFX40). The algorithm is capable of handling multiple primitives made up a set of variables. These variables are built from the strings stored within the facsimile terminal when manufactured and from the public facsimile numbers of the sender and receiver. Using the primitive constructed by these variables and the HKM algorithm a facsimile message can be transmitted securely from sender to receiver. As stated in the contribution, the purpose of HKM is to allow two terminals with hidden and unknown variables in each to send and receive secure messages. In order to achieve this, the terminals must develop some mutual secret (e.g. the above primitive) so that their message cannot become known to a third party. This mutual secret (primitive) is developed during the above mentioned registration procedure.

In addition, the contribution explains that the HFX40 encryption algorithm is based on a 40 bit key which will satisfy the requirements of some Government agencies which maintain security of state for various countries (e.g. U.S.). It also states that a 40 bit key is considered strong enough for all commercial applications but that the algorithm can accommodate other key strengths, for example HFX32, HFX48 or HFX56. The conclusion of the recommendation is that the HKM system should be adopted by Study Group 8 to provide security within Group 3 facsimile.

4.2 COM 8-60

COM 8-60, "Proposed Security System for Group 3 Facsimile" is a detailed description of the registration and automatic modes required by the HKM system. The registration mode is the means by which the MUTUAL PRIMITIVE is generated and transferred between the sending and receiving terminals in a secure manner. The automatic mode is the mode used for the actual transmission of the encrypted

message between the sender and receiver using the predefined MUTUAL PRIMITIVE.

4.2.1 Registration Mode

The operation of registration mode is as follows:

- In a secure environment outside the actual transmission, the sender and receiver agree on a 6 digit secret one-time key.
- Using the UNIQUE IDENTITY STRING and the UNIQUE CRYPT STRING embedded within the facsimile terminal by the manufacturer and the last 6 digits of the sender's and receiver's facsimile numbers a 64 digit primitive of HKM is formed. The UNIQUE CRYPT STRING is then encrypted using the 64 digit primitive generating the 16 digit MUTUAL PRIMITIVE.
- The MUTUAL PRIMITIVE is encrypted using the 6 digit one-time key and is sent to the receiving terminal in the form of a 19 digit TRANSFER KEY.
- The receiver using the one-time key as primitive decrypts the TRANSFER KEY to recover the MUTUAL PRIMITIVE.
- The receiver then encrypts the MUTUAL PRIMITIVE using its own 64 digit primitive comprised of its UNIQUE IDENTITY STRING, UNIQUE CRYPT STRING, and the last 6 digits of the sender's and receiver's facsimile numbers.
- The output of this encryption is a REGISTERED CRYPT STRING that the receiver sends to the sender for use in subsequent "automatic" transmissions.

Shown in Figure 4.1 is the flow diagram of the registration process. Items marked with an "*" are retained within the facsimile machine. Once the MUTUAL PRIMITIVE has been defined, the HKM algorithm provides the means for the selection of a secret session key and the method by which the key is sent to the receiving terminal. This registration process defines a MUTUAL PRIMITIVE for one direction only and must be repeated for the reverse direction.

REGISTRATION

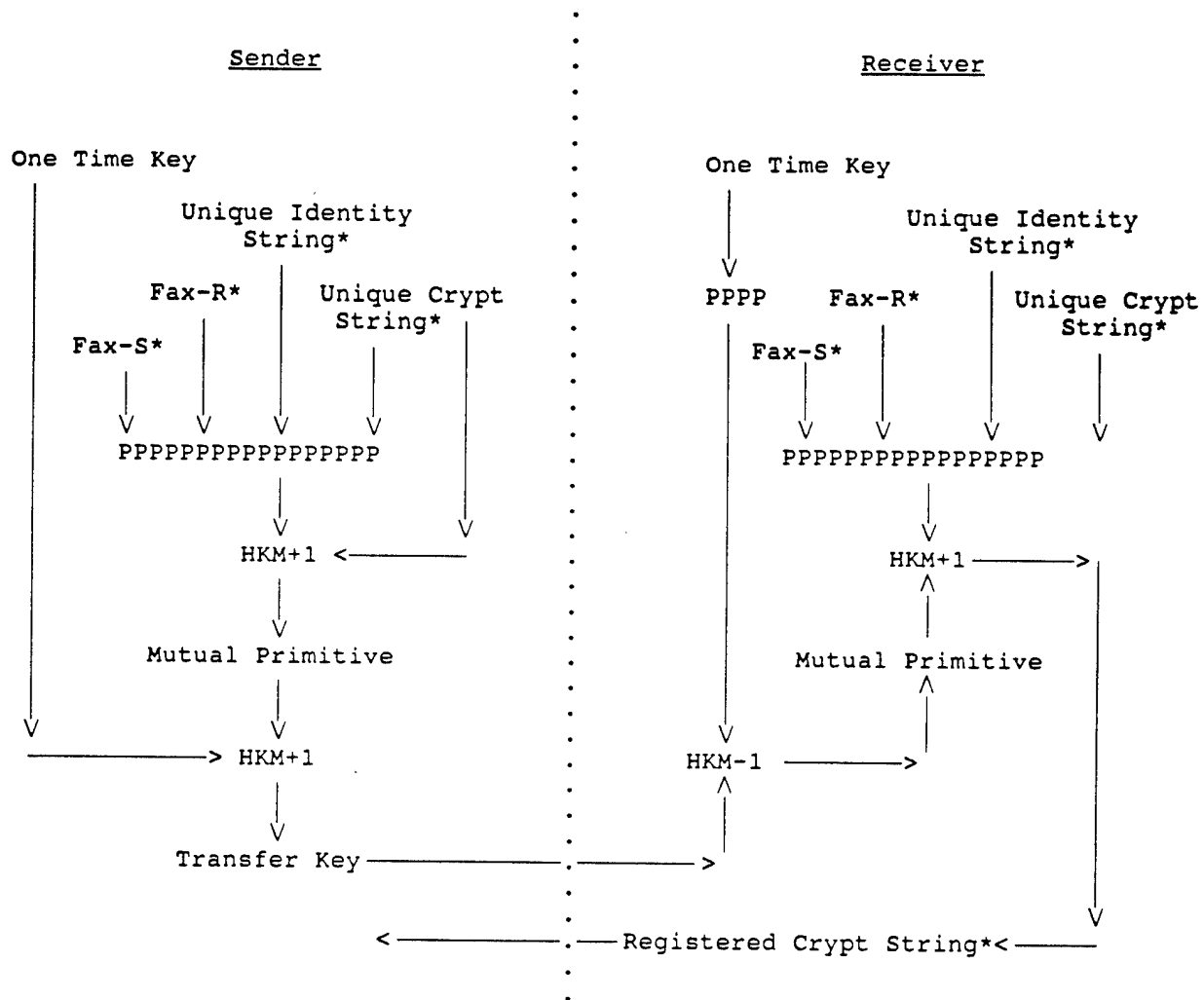


FIGURE 4.1

4.2.2 Automatic Mode

Automatic mode is the mode used for the actual transmission of the encrypted document. Using the MUTUAL PRIMITIVE defined during the registration mode the transmission of the document proceeds as follows:

- Sender recreates the MUTUAL PRIMITIVE.
- Sender creates a 12 digit random session key.
- The random session key is encrypted using the MUTUAL PRIMITIVE.
- The encrypted session key and the REGISTERED CRYPT STRING are sent to the receiving terminal within the T.30 protocol.
- The receiving terminal decrypts the REGISTERED CRYPT STRING using its 64 digit primitive recreating the MUTUAL PRIMITIVE.
- The receiving terminal then decrypts the encrypted random session key with the MUTUAL PRIMITIVE.
- The receiving and sending terminal now both have the session key and the encrypted document can be exchanged securely.

Shown in Figure 4.2 is the flow diagram of the automatic mode. Items marked with an "*" are retained within in the facsimile machine.

As with COM 8-59, this contribution recommended the use of the HKM Encryption System for Group 3 facsimile. It also mentioned that the HKM System is patented. Chantilly Corporation LTD, the holder of the patent, has subsequently submitted TD 3094 to Study Group 8 stating their willingness to conform to Section 2.2 of the TSB Patent Policy.

4.3 COM 8-61

COM 8-61, "Incorporation of Security Features into Recommendation T.30" describes how the registration mode and automatic mode required for the HKM system can be incorporated into Recommendation T.30. The contribution also discusses the limiting of local access to received messages. The following sections detail the contents of the contribution.

4.3.1 Changes to Recommendation T.30

In this contribution it was proposed that two additional bits be added in the Digital identification signal (DIS) and Digital transmit command (DTC) to indicate that a terminal has security capabilities and also the ability to store messages, limiting local access. The associated bit in Digital command signal (DCS) would be used to indicate the activation of the corresponding feature.

AUTOMATIC MODE

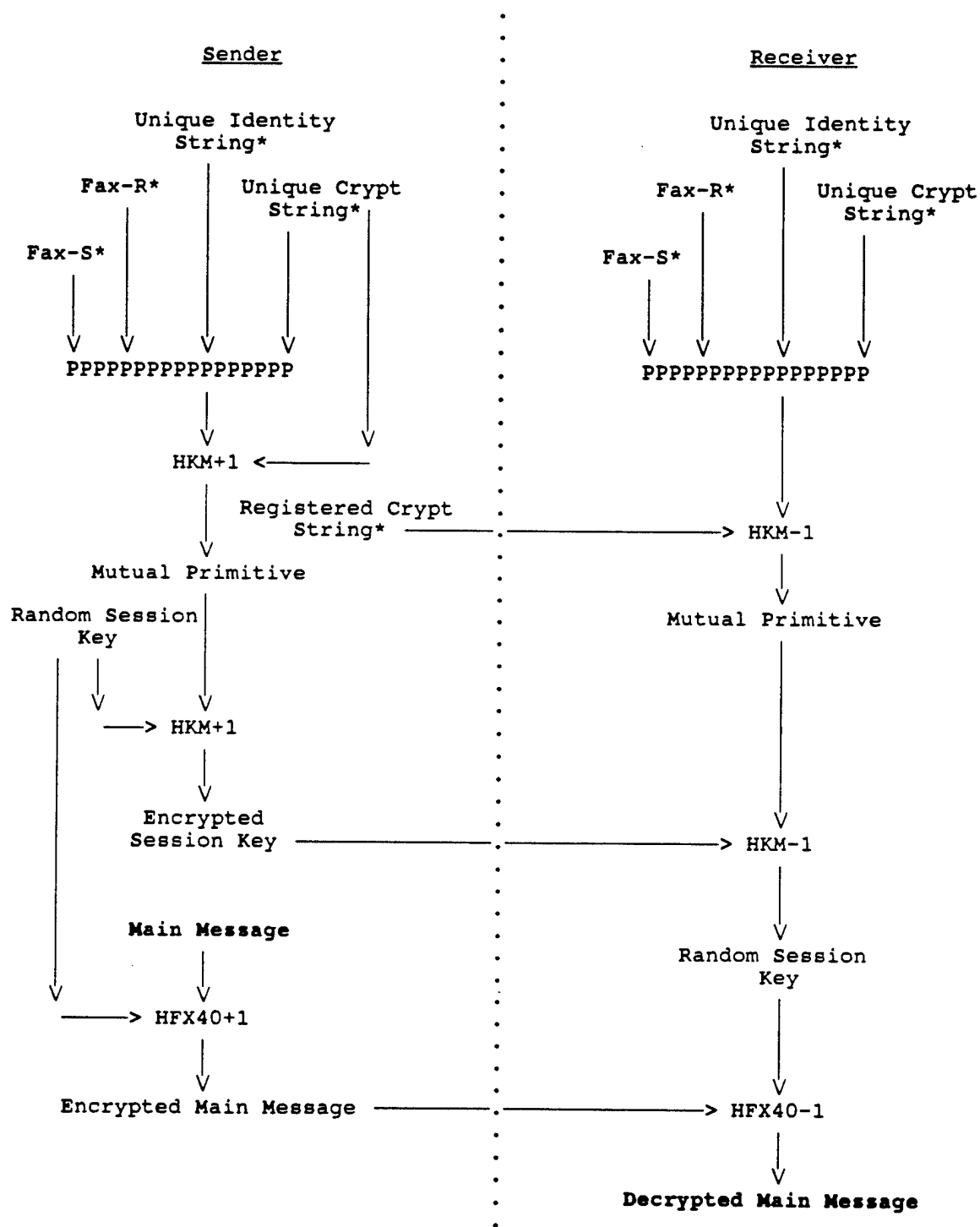


FIGURE 4.2

4.3.2 Registration Mode

Registration mode requires the manual entry of a one time key previously agreed to by the sender and receiver. Since the entry of this key and the initiation of registration mode is manufacturer dependent, it was stated that this was outside the scope of ITU Recommendation. It was suggested that the call be initiated in the normal way with the Transfer Key being sent in coded character mode. Similarly the Registered Crypt String would be sent from the receiver to the sender in coded character mode.

4.3.3 Automatic Mode

This mode requires the transmission of the Registered Crypt String and the Encrypted Session key prior to the message. It was proposed that the Registered Crypt String be sent in the Password information field and the Encrypted Session Key be sent in the sub-address information field. The encryption bit being set in the DCS would tell the receiving terminal that security was being used and to interpret the field accordingly.

4.3.4 Local Access

When the appropriate bit is set in the DIS, the receiver indicates that it has the ability to save messages into a memory store that will not be displayed until the intended recipient retrieves it. In the DCS, the setting of the corresponding bit indicates to the receiver that the message is to be held in memory. The contribution indicated that the actual operation and instructions required to use the message store feature were outside the scope of ITU Recommendations.

4.4 Delayed Contributions D152 and D153 to Study Group 8

In support of COM 8-59, COM 8-60 and COM 8-61, The United Kingdom submitted delayed contributions D152 and D153. Delayed contribution D152, "Details of the HKM Algorithm and Example of Its Use", describes the HKM key-management algorithm and its use. Delayed contribution D153, "Proposed Security System for Group 3 Facsimile - The HFX40 Algorithm", describes the HFX40 message encryption algorithm and its use. With these contributions, the details of the algorithms can be studied to insure that they will fulfill the security requirements of Group 3 facsimile. These delayed contributions have been included in Appendix A.

5.0 CONFIDENTIALITY, KEY MANAGEMENT AND AUTHENTICATION SYSTEM FOR AUDIOVISUAL SERVICES - STUDY GROUP 15 CONTRIBUTIONS

In 1994, a series of contributions from the United Kingdom discussing security in facsimile have been submitted to Study Group 8. Three Contributions, COM 8-59, COM 8-60 and COM 8-61 were discussed in detail in the previous section. In contrast to the contributions submitted by France Telecom, which did not address the specific algorithms to be used to achieve secure facsimile services, these contributions outline a specific approach to the exclusion of others. In response to the U.K. contributions, Siemens submitted delayed contribution D191, "Comments to Incorporation of Security Features into facsimile GR.3". This contribution mentioned the similarities between work being done within Study Group 8 regarding security requirements for Group 3 facsimile and work within Study Group 15 regarding security requirements for audiovisual services. This section will review the two recommendations adopted by Study Group 15, ITU-T H.233 - "Confidentiality System for Audiovisual Services" and ITU-T H.234 - "Encryption Key Management and Authentication System for Audiovisual Services.

5.1 Confidentiality System for Audiovisual Services - H.233

A privacy system consists of two parts, the confidentiality mechanism or encryption process for the data, and a key management subsystem. Recommendation H.233 describes the confidentiality part of a privacy system suitable for use in audiovisual services conforming to Recommendations H.221, H.230 and H.242. Although a confidentiality system requires the use of an encryption algorithm, H.233 does not specify one. The system allows for more than one specific algorithm. The following reviews the confidentiality system described in H.233.

5.1.1 Characteristics of the System's Confidentiality

The characteristic of the systems confidentiality are as follows:

- Confidentiality is independent of the other services provided by the system. Encryption keys are provided to the system by one of the methods described in the draft Recommendation on Authentication and Key Management (H.234), or may be manually entered.
- Confidentiality is given to user audio, video and data transmissions with all signals encrypted with the same key.
- The system is independent of the encryption algorithm used.

5.1.2 Encryption Algorithm Specification

As mentioned previously, no encryption algorithm is specified in H.233. In H.233 one byte has been defined as an algorithm identification. Currently the following algorithm identifiers are assigned:

- 0 - Not allocated. Reserved for future use.
- 1 - "FEAL" - See Appendix II.1 of H.233
- 2 - "DES" Mode 1 - See Appendix II.2 of H.233
- 3 - "Reserved for "DES" Mode 2 - See Appendix II.2 of H.233
- 4 - "Reserved for "DES" Mode 3 - See Appendix II.2 of H.233
- 5 - B-CRYPT - ISO/IEC 9979 algorithm register no. 0001
- 6 - IDEA - ISO/IEC 9979 algorithm register no. 0002
- 7 - BARAS (ETSI) - ISO/IEC 9979 algorithm register no. xxxx

Other values are reserved for future use.

5.2 Encryption Key Management and Authentication For Audiovisual Services - H.234

The second part of a privacy system is the key management subsystem. Recommendation H.234 describes authentication and key management methods for a privacy system for use in audiovisual services conforming to ITU Recommendations H.221, H.230 and H.242. As is stated in H.234, privacy is achieved by the use of secret keys. The keys are loaded into the confidentiality part of the privacy system and control the way in which the transmitted data is encrypted and decrypted. If a third party gains access to the keys being used then the privacy system is no longer secure. The handling/maintenance of keys by the users is thus an important part of any privacy system. Three methods of encryption key management are described in H.234: ISO 8732, Diffie-Hellman and RSA. Additionally, for cases where automated key management is not practical, an alternative such as manual key management can be used. The following reviews each of the encryption methods.

5.2.1 ISO 8732

ISO 8732 is based on manually installed keys in systems that provide a high measure of protection, and then an automated exchange of keys encrypted under the manually distributed keys. The algorithm used for encrypting the automatically distributed keys is usually the same as that used to encrypt the message itself. The security of the automatically distributed keys is directly dependent on the security of the manually distributed keys.

The automatically distributed keys may be used for a single session, or for multiple sessions in a given time period (e.g. a month). ISO 8732 contains protocols not only for the automated exchange of information between the two terminals, but also physical protocols for ensuring the security of the manual distribution of keys as well.

5.2.2 Extended Diffie-Hellman

Extended Diffie-Hellman is a simple yet secure method of key management which generates and exchanges keys automatically via the system itself (this key exchange is itself encrypted). It requires no action from the users until the keys have been exchanged; at which point they are asked to confirm verbally that the same check sequence is displayed at each terminal. This method is more than sufficient to prevent outsiders from listening in on an audiovisual call carried over a satellite channel. To defeat the system, it would be necessary for a third party to intercept completely the bi-directional communication before encryption has been activated, and to exchange keys with both parties, pretending to each that it is the other legitimate party. As was stated in Section 4.1.1, the Diffie-Hellman method does not provide authentication.

5.2.3 RSA Method

The third method specified in H.234 is the "RSA Method" and is very similar to the public key method specified in Recommendation X.509 and uses the RSA algorithm. The RSA algorithm was developed by Ron Rivest, Adi Shamir, and Leonard Adleman as a public-key cryptosystem for both encryption and authentication. A public-key cryptosystem (or asymmetric system) is one where each user has a pair of keys: a public key and a private key. A user's public key can be freely distributed or stored in a global directory for general use. The private key is known only to the individual user. Within the RSA method of key management a session key is exchanged between the two users by encrypting it with a user's public key and transmitting it to the receiving terminal. The receiving terminal then decrypts the session key using their private key. The use of the RSA Method also provides for authentication.

The RSA method does require the establishment of a security agency (Certification Authority) that is available to all users who wish to communicate with each other. This agency would probably be a multi level entity existing at the local, national and global levels. The certification process is done "off-line" and relies on the integrity of the agency. This authentication/certification process allows the parties involved to be identified to each other in an assured manner, and can be operated in multipoint as well as point-to-point calls.

5.2.4 Manual Key Exchange

Manual key exchange is defined as the user entering Key Encryption Keys directly into terminals without message exchanges within the protocol being used. The same key is entered at both locations. The key length is encryption algorithm dependent. The actual method for entering the keys into the terminal is terminal dependent, but could be as simple as using a telephone keypad to enter the binary bit pattern of the encryption key.

Manual entry of the key may occur prior to initiating the call, or while the call is in progress. The users may decided to invoke encryption while in a conference, enter a key using the interface provided by the terminal, and then begin encryption through the terminal's user interface.

6.0 SUMMARY AND RECOMMENDATIONS

6.1 Summary

Temporary Document 3081, a liaison statement from Study Group 1 to Study Group 8, specified the following security services as required services for Group 3 and 4 facsimile.

- Authentication of sending machine
- Authentication of sending human
- Authentication of receiving machine
- Authentication of receiving human
- Message Integrity
- Protection against replay
- Confidentiality on line
- Local access to messages

Based on a review of all contributions to Study Group 8 regarding security services for Group 3 and Group 4 facsimile, the approach outlined in COM 8-30 and it's subsequent supporting documents from France Telecom best meet the above listed requirements. These documents address both Group 3 and Group 4 implementations and do not limit the encryption method used to achieve the required services. In various documents, specifically D191 from DBP Telekom, Germany and D199 from Siemens, the use of a specific encryption algorithm, as proposed by the U.K contributions, is questioned. The approach of France Telecom allows the specification of the encryption algorithm to be negotiated within the protocol the same as is done in Recommendation H.234 for Audiovisual Services. This approach allows for encipherment issues to be handled on a national basis. As was noted in D191, this approach allows the use of the HKM System along with RSA or Diffie-Hellman for key management if users require it. Additionally it is not clear how authentication of sending and receiving humans can be achieved in the proposed Group 3 implementation of the HKM system.

6.2 Recommendations

There are various ongoing activities within the United States regarding encryption that could impact Group 3 and Group 4 facsimile. Congressional hearings, both in the senate and the house, were begun addressing the status of the clipper chip. The administration would like the clipper chip to be a national standard for encryption. This has caused a great deal of controversy within the encryption community primarily because of the escrowing of the encryption keys with a government agency so that they can be retrieved by law enforcement officials for surveillance activities. In addition, a bill was introduced by Rep Maria Cantwell from Washington, HR 3627 - Cantwell Cryptography Export Bill, that would loosen controls on the export of encryption software. Currently most encryption technology beyond a certain strength (greater than 40 bit encryption keys) cannot be exported from the U.S. Because of this limitation, software and hardware products must be built with an "inferior" encryption technology if they

are to be exported. U.S. manufacturers maintain that they cannot compete in a global market with this limitation. The administration is currently reviewing all encryption regulations. Until the review is complete, all export regulations remain in place. Both these activities should be monitored during the next year.

As was detailed in this report, there is a significant amount of work going on within ITU Study Group 8 with regard to secure facsimile. Since the ITU issues all recommendations governing the use and implementation of facsimile on the international level, all activities should be monitored. Specifically, Study Group 8 has established a list of 13 questions regarding security (TD 3140). It has requested contributions answering these questions. All contributions submitted to Study Group 8 in response to these questions should be reviewed.

REFERENCES

- [1] National Communications System, *Security and Facsimile*, NCS TIB 93-16, December 1993.
- [2] W. Diffie and M.E. Hellman. New directions in cryptography. IEEE Transactions on Information Theory, IT-22(6), Nov. 1976, pp. 644-654.

APPENDIX A

UIT - Secteur de la normalisation des télécommunications
ITU - Telecommunication Standardization Sector
UIT - Sector de Normalización de las Telecomunicaciones

Commission d'études }
Study Group } **8**
Comisión de Estudio }

Contribution tardive }
Delayed Contribution }
Contribución tardía }

D 152/T

Geneva, 21 - 30 June 1994

Question : 5/8

Texte disponible seulement en }
Text available only in } **E**
Texto disponible solamente en }

Source : United Kingdom

Title : Details of the HKM Algorithm and Examples of Its Use

1. Introduction

Contributions COM 8-59 and COM 8-60 refer to two cipher algorithms HKM and HFX40. These algorithms are based on the same principles but are used in different manners, with different parameters. The HKM algorithm is used for secure key transfer and HFX40 is used for the secure transfer of the main facsimile message. This paper describes the HKM key-management algorithm and its use.

2. Background

The encryption algorithm uses a number of machine-specific identifiers or primitives, and an encryption key to provide the input numbers for calculations using modular arithmetic. The modulus for the modular arithmetic are provided by a number of special prime numbers. The output of the modular arithmetical processes is an extremely long, irreversible pseudo random sequence, (PRS), that is combined with the message. Only by possessing the key is it possible to recreate the message.

This results in secure transfer of the Mutual Primitive during Registration Mode and of the Session Key during Automatic Mode.

3. The HKM Algorithm

The HKM algorithm describes the rules for the computations carried out using these numbers during the Registration Mode and Session Key transfer. The rules are best explained using numerical examples.

Contact person - Name: Mr A T Bence, U.K.

Tel: +44 473 640 891

Fax: +44 473 640 897

3.1 Stored information

The HKM algorithm requires some information to be stored in each facsimile machine.

All machines are equipped with the same 19 prime numbers

| | | | | | | | | | |
|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| 32603 | 32507 | 32183 | 32003 | 31847 | 31607 | 31583 | 31547 | 31259 | 31139 |
| 30803 | 30539 | 30467 | 30347 | 30323 | 30203 | 29879 | 29759 | 29663 | |

The 19 prime numbers are included to give an increased range of selection for the secure transfer of the document using the HFX40 algorithm which is described in COM 8-D

Each machine is also equipped, by some suitable process, with two randomly generated decimal digit numbers. These are the 48 digit Unique Identity String and the 16 digit Unique Crypt String.

For example: Unique Identity String = 345092978336094172898029844342879120988727823781
and Unique Crypt String = 1333908734565521

The Unique Identity String and Unique Crypt String are used with other identifying numbers to form the primitives for the HKM algorithm.

3.2 Registration Mode

The user at the sending facsimile machine selects the Registration Mode and enters the destination address of the receiving facsimile machine with which registration is to take place. The last six digits of the destination address together with the last six digits of the address of the sending machine form the basis of the other identifiers used by the algorithm. The user is also prompted to enter the agreed secret One-Time Key.

3.2.1 The next step is to generate the Transfer Key at the sending terminal and send it to the receiving terminal. This is generated using the telephone numbers of the sending and receiving machines, the One-Time Key, the Unique Identity String and Unique Crypt String plus the first nine prime numbers, as explained below.

| | | |
|-------------|---------------------------------------|----------|
| For example | Last six digits of sender's address | = 642092 |
| | Last six digits of receiver's address | = 538249 |
| | Secret One-Time key | = 582617 |

The basic algorithm uses the primes as moduli for performing modular arithmetic using phase and base numbers. Modular arithmetic is used to limit the size of the numbers generated. The phase and base numbers are generated as follows:

A 64 digit primitive is formed by concatenating the Unique Identity String and Unique Crypt String.

This primitive is then split into two 32bit strings and the phase values (P(0) to P(8)) are obtained from the first 32bits and the B values (B(0) to B(8)) are obtained from the second 32bits. The phase values are derived by dividing the first 32bits into 7 sets of 4 digits and 2 sets of 2 digits. The base values are derived in exactly the same way from the second 32bits.

The P values are modified by adding incremental products of 101 and the B values are modified by adding incremental products of 79. The modification by 101 and 79 is used to ensure that modulation by the prime number starts as soon as possible.

- 3 -

Using the examples above the P and B values are derived as shown below.

Expanded Primitive = 3450929783360941728980298443428791209887278237811333908734565521

| | | | |
|------|-------------------------|------|------------------------|
| P(0) | $3450 + 0 * 101 = 3450$ | B(0) | $9120 + 0 * 79 = 9120$ |
| P(1) | $9297 + 1 * 101 = 9398$ | B(1) | $9887 + 1 * 79 = 9966$ |
| P(2) | $8336 + 2 * 101 = 8538$ | B(2) | $2782 + 2 * 79 = 2940$ |
| P(3) | $941 + 3 * 101 = 1244$ | B(3) | $3781 + 3 * 79 = 4018$ |
| P(4) | $7289 + 4 * 101 = 7693$ | B(4) | $1333 + 4 * 79 = 1649$ |
| P(5) | $8029 + 5 * 101 = 8534$ | B(5) | $9087 + 5 * 79 = 9482$ |
| P(6) | $8443 + 6 * 101 = 9049$ | B(6) | $3456 + 6 * 79 = 3930$ |
| P(7) | $42 + 7 * 101 = 749$ | B(7) | $55 + 7 * 79 = 608$ |
| P(8) | $87 + 8 * 101 = 895$ | B(8) | $21 + 8 * 79 = 653$ |

The six digit components of the sender's and receiver's telephone numbers are split into two three digit groups. These are used to modify the first four values of P(0) to P(3) to give new values to P(0) to P(3).

$$\begin{aligned} P(0) &= 3450 + 642 = 4092 \\ P(1) &= 9398 + 092 = 9490 \\ P(2) &= 8538 + 538 = 9076 \\ P(3) &= 1244 + 249 = 1493 \end{aligned}$$

3.3 Calculation of the Mutual Primitive

The 9 primes, the 9 P values and the 9 B values are used according to the HKM algorithm to generate a pseudo random sequence (PRS) of numbers (mod 10). One number is generated per digit of the 'message', which for Registration Mode is the Unique Crypt String. The PRS is added (mod 10) to the Unique Crypt String to form the Mutual Primitive.

3.3.1 Example Calculations to Form the Mutual Primitive

Modular arithmetic is carried out using sets of a prime number and a P and a B value. The prime number being used as the modulus.

For example, for the first set ie P(0), B(0) and the first prime number:

$$\begin{aligned} P(0) &\text{ is multiplied by } B(0) \\ 4092 * 9120 &= 37319040 \\ 37319040 \text{ (mod the first prime)} &= 37319040 \text{ (mod 32603)} = 21208 \end{aligned}$$

$$\begin{aligned} 21208 &\text{ is then used as the new phase value and is multiplied by the base value (B(0))} \\ 21208 * 9120 &= 193416960 \\ 193416960 \text{ (mod the first prime)} &= 193416960 \text{ (mod 32603)} = 15964 \end{aligned}$$

This process is carried out a total of 16 times (corresponding to the number of digits in the Unique Crypt String). It is also repeated for the remaining 8 sets of primes, base and phase values.

The results of the first calculation for each of the 9 prime, B and P "sets" are added. The result is added (modulo 10) to the first digit of the Unique Crypt String to form the first digit of the Mutual Primitive. The process is repeated for each digit of the Unique Crypt String.

Table 1 shows the results of the above operations to produce the Mutual Primitive 6882213309628039 from the Unique Crypt String.

- 5 -

$$\begin{aligned} P(7) & 17 + 7 * 101 = 724 \\ P(8) & 58 + 8 * 101 = 866 \end{aligned}$$

$$\begin{aligned} B(7) & 58 + 7 * 79 = 611 \\ B(8) & 26 + 8 * 79 = 658 \end{aligned}$$

The P and B values are then used together with the prime numbers as before to derive the Mutual Primitive.

The Mutual Primitive = 6882213309628039 is recovered as shown in Table 3.

5. Creation of the Registered Crypt String

5.1 Following the same procedures as detailed in 3, the receiver splits and modifies its own 48 digit Unique Identity String and the 16 digit Unique Crypt String to form the P and B values. The last 6 digits from the telephone numbers of sender and of the receiving machine are used with the P and B numbers as before. These are used following the rules of the HKM algorithm as described in 3 above to develop a PRS which can be added to the Mutual Primitive. This encrypted Mutual Primitive is the Registered Crypt String which can be communicated openly. It does not need to be stored at the receiver but is sent back to the sender. It is used by the sender when communicating with this receiver when working in the encrypted mode.

5.1.1 Generation of P values and B values

Unique Identity String = 973557693837783148353709167436722873449819767357

Unique Crypt String = 7598247578649467

Expanded primitive = 9735576938377831483537091674367228734498197673577598247578649467

$$\begin{aligned} P(0) & 9735 + 0 * 101 = 9735 \\ P(1) & 5769 + 1 * 101 = 5870 \\ P(2) & 3837 + 2 * 101 = 4039 \\ P(3) & 7831 + 3 * 101 = 8134 \\ P(4) & 4835 + 4 * 101 = 5239 \\ P(5) & 3709 + 5 * 101 = 4214 \\ P(6) & 1674 + 6 * 101 = 2280 \\ P(7) & 36 + 7 * 101 = 743 \\ P(8) & 72 + 8 * 101 = 880 \end{aligned}$$

$$\begin{aligned} B(0) & 2873 + 0 * 79 = 2873 \\ B(1) & 4498 + 1 * 79 = 4577 \\ B(2) & 1976 + 2 * 79 = 2134 \\ B(3) & 7357 + 3 * 79 = 7594 \\ B(4) & 7598 + 4 * 79 = 7914 \\ B(5) & 2475 + 5 * 79 = 2870 \\ B(6) & 7864 + 6 * 79 = 8338 \\ B(7) & 94 + 7 * 79 = 647 \\ B(8) & 67 + 8 * 79 = 699 \end{aligned}$$

5.1.2 P(0), P(1), P(2) and P(3) are then modified as before by the last six digits of the sending and receiving machine telephone numbers.

Last six digits of sender's address = 642092

Last six digits of receiver's address = 538249

$$\begin{aligned} P(0) & = 9735 + 642 = 10377 \\ P(1) & = 5870 + 092 = 5962 \\ P(2) & = 4039 + 538 = 4577 \\ P(3) & = 8134 + 249 = 8383 \end{aligned}$$

5.1.3 The P and B values are then used in conjunction with the prime numbers in exactly the same way as before to generate a PRS. The PRS is then added (mod 10) to the Mutual Primitive to obtain the Registered Crypt String.

Table 4 shows the results of calculations to produce the Registered Crypt String from the Mutual Primitive.

The Registered Crypt String 0060055468650340 is sent to the sending machine where it is stored associated with the receiving machine address.

6. THE USE OF THE HKM ALGORITHM IN AUTOMATIC MODE

The HKM algorithm is used in Automatic Mode to re-create the Mutual Primitive at both sending and receiving machine and to securely transfer the Random Session Key to be used to encrypt the main Facsimile message

The rules of the algorithm are however exactly the same as those previously described for Registration Mode, Paras 3. and 4 above.

6.1 Use at the Sending Machine

To send a message securely the user at the sending machine enters the destination address with which registration has been carried out.

6.1.1 Recalculation of the Mutual Primitive

To re-create the Mutual Primitive the same prime numbers, primitives and modifiers are used. The last 6 digits of the address are used exactly as during the original Registration Mode (see Table 1).

6.1.2 The sending machine generates a 12 digit Random Session Key and a four digit Random String for each call. The HKM algorithm is used with the Random String and the recreated Mutual Primitive to encrypt the Random Session Key. This procedure is shown below assuming a Random String 3958 and a Random Session Key 757844059916.

6.1.3 Calculation of the Encrypted Session Key

6.1.4 Calculation of the P and B Values.

Expanded primitive (by repeating the Mutual Primitive) =

6882213309628039688221330962803968822133096280396882213309628039

| | | | |
|------|-----------------------------|------|----------------------------|
| P(0) | $6882 + 0 \cdot 101 = 6882$ | B(0) | $6882 + 0 \cdot 79 = 6882$ |
| P(1) | $2133 + 1 \cdot 101 = 2234$ | B(1) | $2133 + 1 \cdot 79 = 2212$ |
| P(2) | $962 + 2 \cdot 101 = 1164$ | B(2) | $962 + 2 \cdot 79 = 1120$ |
| P(3) | $8039 + 3 \cdot 101 = 8342$ | B(3) | $8039 + 3 \cdot 79 = 8276$ |
| P(4) | $6882 + 4 \cdot 101 = 7286$ | B(4) | $6882 + 4 \cdot 79 = 7196$ |
| P(5) | $2133 + 5 \cdot 101 = 2638$ | B(5) | $2133 + 5 \cdot 79 = 2528$ |
| P(6) | $962 + 6 \cdot 101 = 1568$ | B(6) | $962 + 6 \cdot 79 = 1436$ |
| P(7) | $80 + 7 \cdot 101 = 787$ | B(7) | $80 + 7 \cdot 79 = 633$ |
| P(8) | $39 + 8 \cdot 101 = 847$ | B(8) | $39 + 8 \cdot 79 = 671$ |

6.1.5 The Random String is divided into 2 sets of 2 digits and the first set is added to P(0) and the second set to P(1):-

$$\begin{aligned} P(0) &= 6882 + 39 = 6921 \\ P(1) &= 2234 + 58 = 2292 \end{aligned}$$

6.1.6 The prime numbers, P and B values are then used in exactly the same way as before to generate a 12 digit PRS. Table 5 shows the results of the calculations to produce the encrypted session key.

6.1.7 The sending machine sends the Registered Crypt String, the Random String and the Encrypted Session Key to the receiving machine.

Registered Crypt String = 0060055468650340
Random String = 3958
Encrypted Session Key = 359104518785

- 7 -

6.2 Use at the Receiving Machine

6.2.1 The receiving machine decrypts the Registered Crypt String using the HKM algorithm and the P and B values derived from its own primitives and the last 6 digits from the telephone numbers of the sender and receiver as it did when originally encrypting it as in Section 5. Decryption provides the receiver with the Mutual Primitive (see Table 6).

6.2.2 The Mutual Primitive is then used to recreate the Session Key:-

The Mutual Primitive is concatenated to give 64 digits from which P and B values are derived as before.

Random String = 3958
 Encrypted session key = 359104518785
 Expanded primitive = 6882213309628039666221330962803966622133096280396662213309628039

| | | | |
|------|-----------------------------|------|----------------------------|
| P(0) | $6882 + 0 \cdot 101 = 6882$ | B(0) | $6882 + 0 \cdot 79 = 6882$ |
| P(1) | $2133 + 1 \cdot 101 = 2234$ | B(1) | $2133 + 1 \cdot 79 = 2212$ |
| P(2) | $962 + 2 \cdot 101 = 1164$ | B(2) | $962 + 2 \cdot 79 = 1120$ |
| P(3) | $8039 + 3 \cdot 101 = 8342$ | B(3) | $8039 + 3 \cdot 79 = 8276$ |
| P(4) | $6882 + 4 \cdot 101 = 7286$ | B(4) | $6882 + 4 \cdot 79 = 7198$ |
| P(5) | $2133 + 5 \cdot 101 = 2638$ | B(5) | $2133 + 5 \cdot 79 = 2528$ |
| P(6) | $962 + 6 \cdot 101 = 1568$ | B(6) | $962 + 6 \cdot 79 = 1436$ |
| P(7) | $80 + 7 \cdot 101 = 787$ | B(7) | $80 + 7 \cdot 79 = 633$ |
| P(8) | $39 + 8 \cdot 101 = 847$ | B(8) | $39 + 8 \cdot 79 = 671$ |

Modification of P(0) and P(1):-

P(0) = $6882 + 39 = 6921$
 P(1) = $2234 + 58 = 2292$

Using sets of primes, P and B values a PRS is produced which is subtracted mod (10) from the 12 digit encrypted session key to recreate the session key (see Table 7).

6.3 Once the Session Key has been securely exchanged the system is ready to securely transfer the main message using the Session Key with the HFX40 algorithm. For details of this algorithm and examples of its use see the COM 8-Delayed Contribution D. 153

TABLE 1

Creation of Mutual Primitive

| Prime B(n) | 32603 | 32507 | 32183 | 32003 | 31847 | 31607 | 31583 | 31547 | 31259 | LAST | | | CRYPT | | | MUTUAL | | |
|---------------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|--------|-----------|--------|-----------|--------|-----------|---|--|
| | | | | | | | | | | DIGIT | STRING | PRIMITIVE | STRING | PRIMITIVE | STRING | PRIMITIVE | | |
| P(n) | 9120 | 9966 | 2940 | 4018 | 1649 | 9482 | 3930 | 608 | 653 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | 1 | |
| | 4092 | 9490 | 9076 | 1493 | 7693 | 8534 | 9049 | 749 | 895 | 5 | 3 | 5 | 3 | 5 | 3 | 5 | 3 | |
| | 21208 | 14481 | 3733 | 14313 | 10651 | 5472 | 110 | 13734 | 21773 | 9 | 3 | 9 | 3 | 9 | 3 | 9 | 3 | |
| | 15964 | 19075 | 617 | 241 | 15803 | 18417 | 21721 | 21864 | 26183 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | |
| | 19285 | 520 | 11732 | 8248 | 8302 | 1325 | 26262 | 12025 | 30086 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | |
| | 18618 | 13707 | 24087 | 17359 | 27635 | 15671 | 28003 | 23843 | 15506 | 3 | 9 | 3 | 9 | 3 | 9 | 3 | 9 | |
| | 32339 | 9554 | 13176 | 13927 | 28906 | 7909 | 16620 | 16471 | 28761 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | |
| | 4942 | 2165 | 21291 | 17444 | 22880 | 21332 | 2956 | 13969 | 25532 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | |
| | 13694 | 24249 | 31788 | 3422 | 22272 | 16823 | 26119 | 7009 | 11349 | 5 | 8 | 5 | 8 | 5 | 8 | 5 | 8 | |
| | 19780 | 8498 | 29471 | 20309 | 6937 | 28758 | 2922 | 2627 | 2514 | 6 | 7 | 6 | 7 | 6 | 7 | 6 | 7 | |
| | 27195 | 10337 | 8100 | 25913 | 6040 | 9971 | 18831 | 19866 | 16174 | 7 | 3 | 7 | 3 | 7 | 3 | 7 | 3 | |
| | 7379 | 3861 | 30763 | 12673 | 23696 | 8487 | 6863 | 27574 | 27339 | 5 | 4 | 5 | 4 | 5 | 4 | 5 | 4 | |
| | 3688 | 22947 | 8986 | 3339 | 30282 | 2314 | 31291 | 13535 | 3479 | 1 | 5 | 1 | 5 | 1 | 5 | 1 | 5 | |
| | 19099 | 3063 | 28780 | 6845 | 30767 | 6090 | 21013 | 27060 | 21139 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | |
| | 17654 | 1765 | 4093 | 12633 | 2513 | 30998 | 23126 | 16493 | 18548 | 3 | 5 | 3 | 5 | 3 | 5 | 3 | 5 | |
| | 10866 | 7981 | 29161 | 2634 | 3827 | 9547 | 20893 | 27345 | 14611 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | |
| | 17403 | 26526 | 30015 | 22422 | 5017 | 2208 | 25271 | 491 | 6988 | 1 | 2 | 1 | 2 | 1 | 2 | 1 | 2 | |
| | 3566 | 11188 | 30493 | 3155 | 24650 | 12422 | 18080 | 14605 | 30609 | 8 | 1 | 8 | 1 | 8 | 1 | 8 | 1 | |

Mutual primitive 8882213309628039

[illegible]

Mutual primitive = 6082213300028039

TABLE 5

Creation of Encrypted Session Key

| Prime | Session Key | | | | | | | | | | LAST DIGIT | ENCRYPTED | |
|-------|-------------|-------|-------|-------|-------|-------|-------|-------|-------|----------------|---------------|----------------|--|
| | 32503 | 32507 | 32183 | 32003 | 31847 | 31607 | 31583 | 31547 | 31259 | SESSION KEY | | SESSION KEY | |
| B(n) | 6882 | 2212 | 1120 | 8276 | 7198 | 2528 | 1436 | 633 | 671 | 6 | 7 | 3 | |
| P(n) | 6921 | 2292 | 1164 | 8342 | 7286 | 2638 | 1568 | 787 | 847 | 0 | 5 | 5 | |
| | 29940 | 31319 | 16360 | 7921 | 24466 | 31394 | 9255 | 24966 | 5675 | 181296 | | | |
| | 28715 | 5215 | 11073 | 12052 | 24209 | 30462 | 25320 | 29978 | 25586 | 192610 | | | |
| | 9841 | 28102 | 11305 | 21004 | 21447 | 13284 | 7487 | 16327 | 7015 | 135812 | | | |
| | 9329 | 8240 | 13681 | 20811 | 13095 | 15318 | 13112 | 19122 | 18215 | 130923 | | | |
| | 6869 | 22980 | 3612 | 23697 | 22535 | 5329 | 5364 | 21725 | 31255 | 143346 | | | |
| | 30709 | 11586 | 22565 | 1984 | 10157 | 7130 | 28035 | 28980 | 28574 | 169720 | | | |
| | 6698 | 12716 | 9145 | 2045 | 21223 | 8650 | 21518 | 15533 | 11387 | 108915 | | | |
| | 27597 | 9237 | 8206 | 26836 | 24940 | 26763 | 11674 | 21272 | 13481 | 170006 | | | |
| | 10085 | 17848 | 18565 | 25919 | 28420 | 17884 | 24874 | 26154 | 11900 | 181649 | | | |
| | 25784 | 16278 | 2582 | 21542 | 13887 | 12742 | 30274 | 24854 | 13855 | 161798 | | | |
| | 19952 | 21687 | 27553 | 24890 | 22738 | 4243 | 15256 | 22176 | 12782 | 171287 | | | |
| | 22041 | 23819 | 28046 | 18074 | 6395 | 11531 | 20597 | 30540 | 11756 | 173049 | | | |

Random string = 3958
Encrypted session key = 359104518785

TABLE 7

Recreation of Session Key

| Prime | 32603 | 32507 | 32183 | 32003 | 31847 | 31607 | 31583 | 31547 | 31259 | ENCRYPTED | | |
|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|---------------|----------------|----------------|
| | | | | | | | | | | LAST DIGIT | SESSION KEY | SESSION KEY |
| B(n) | 6882 | 2212 | 1120 | 8276 | 7198 | 2528 | 1436 | 633 | 671 | 6 | 3 | 7 |
| P(n) | 6921 | 2292 | 1164 | 8342 | 7286 | 2638 | 1568 | 787 | 847 | 0 | 5 | 5 |
| | 29940 | 31319 | 16360 | 7921 | 24466 | 31394 | 9255 | 24966 | 5675 | 181296 | 9 | 7 |
| | 28715 | 5215 | 11073 | 12052 | 24209 | 30462 | 25320 | 29978 | 25586 | 192610 | 2 | 9 |
| | 9841 | 28102 | 11305 | 21004 | 21447 | 13284 | 7487 | 16327 | 7015 | 135812 | 3 | 1 |
| | 9329 | 8240 | 13681 | 20811 | 13095 | 15318 | 13112 | 19122 | 18215 | 130923 | 6 | 0 |
| | 6869 | 22960 | 3612 | 23697 | 22635 | 5329 | 5364 | 21725 | 31255 | 143346 | 0 | 4 |
| | 30709 | 11586 | 22565 | 1984 | 10157 | 7130 | 28035 | 28980 | 28574 | 169720 | 5 | 5 |
| | 6698 | 12716 | 9145 | 2045 | 21223 | 8650 | 21518 | 15533 | 11387 | 108915 | 6 | 1 |
| | 27597 | 9237 | 8206 | 26836 | 24940 | 26763 | 11674 | 21272 | 13481 | 170006 | 9 | 8 |
| | 10085 | 17848 | 18565 | 25919 | 28420 | 17884 | 24874 | 26154 | 11900 | 181649 | 8 | 7 |
| | 25784 | 16278 | 2582 | 21542 | 13887 | 12742 | 30274 | 24854 | 13855 | 161798 | 7 | 1 |
| | 19952 | 21687 | 27553 | 24890 | 22738 | 4243 | 15256 | 22176 | 12782 | 171287 | 9 | 5 |
| | 22041 | 23819 | 28046 | 18324 | 6395 | 11531 | 20597 | 30540 | 11756 | 173049 | 9 | 6 |

SESSION KEY = 757844059916

UIT - Secteur de la normalisation des télécommunications
ITU - Telecommunication Standardization Sector
UIT - Sector de Normalización de las Telecomunicaciones

Commission d'études }
Study Group } **8**
Comisión de Estudio }

Contribution tardive } **D 153/T**
Delayed Contribution }
Contribución tardía }

Geneva, 21 - 30 June 1994

QUESTION : 5/8

Texte disponible seulement en } **E**
Text available only in }
Texto disponible solamente en }

SOURCE : UNITED KINGDOM

TITLE : PROPOSED SECURITY SYSTEM FOR GROUP 3 FACSIMILE
THE HFX40 ALGORITHM

1. INTRODUCTION

ITU Contributions COM 8-59 and COM 8-60 refer to two cipher algorithms HFX40 and HKM. These algorithms are based on the same principles but are used in different manners, with different parameters. The HFX40 is used for the secure transfer of the main facsimile message and the HKM algorithm is used for secure key management. This contribution describes the HFX40 message encryption algorithm and its use.

2. BACKGROUND

The encryption algorithm uses a number of user-specific identifiers or primitive, and an encryption key to provide the input numbers for calculations using modular arithmetic. The moduli for the modular arithmetic are provided by a number of special prime numbers. The output of the modular arithmetical processes are extremely long Pseudo Random Sequences (PRS) that are used to encrypt the message. Only by possessing the encryption key is it possible to recreate the message.

The proposed HFX40 algorithm uses a 12 decimal digit key, approximately equivalent to a key strength of 40 bits. The algorithm is sufficiently flexible to allow other key strengths to be selected if necessary.

Contact person - Mr A T Bence

Tel: +44 473 640 891
Fax: +44 473 640 897

3. THE HFX40 ALGORITHM

The HFX algorithm describes the rules for the computations carried out to provide the PRSs to be used to provide the message encryption and decryption during Automatic Mode. The rules are best explained using numerical examples.

The HFX algorithm uses only the 19 System Modulating Prime Numbers of the information required by the HKM algorithm to be stored in the facsimile machine:

32603, 32507, 32183, 32003, 31847, 31607, 31583, 31547, 31259, 31139
30803, 30539, 30467, 30347, 30323, 30203, 29879, 29759, 29663

4. USE OF THE HFX40 ALGORITHM IN AUTOMATIC MODE

4.1 To send a message securely the user at the sending facsimile machine enters the destination address with which Registration has been carried out. The sending machine sends the Registered Crypt String associated with the receiving machine to the receiving machine. A 12 digit Random Session Key is generated and sent securely to receiving machine encrypted by the HKM algorithm using the Mutual Primitive associated with the receiver as the encryption key. This procedure is explained in detail in COM 8-D. The main facsimile message is encrypted by the HFX40 algorithm using the Session Key and sent to the receiver.

4.2 To match the complexity of the algorithm to the size of the key the HFX40 algorithm does not use as many primes as the HKM algorithm to absorb the key. However to ensure the strength of the encryption, three primes are selected from the 19 stored for each call. The Random Session Key is used to make the selection, as explained in the following sections.

4.3 Selection of Primes

The Random Session Key, for this example 149162536496, is split into four three digit groups.

The value (mod 19) of the first group of digits is used to determine which number prime is exchanged with the first prime in the table of System Modulating Primes. The value (mod 19) of the second group determines which number prime is changed with the second prime and the value (mod 19) of the third group is used to determine which number prime is changed with the third prime. The first prime (32603) is number 0 and the last (29663) is number 18

32603, 32507, 32183, 32003, 31847, 31607, 31583, 31547, 31259, 31139
30803, 30539, 30467, 30347, 30323, 30203, 29879, 29759, 29663

4.3.1 Example of the Calculations to Select primes

Random Session Key = 149 162 536 496. the first three groups only are used

149 (mod 19) = 16, therefore prime 16 is exchanged with prime 0.
29879, 32507, 32183, 32003, 31847, 31607, 31583, 31547, 31259, 31139
30803, 30539, 30467, 30347, 30323, 30203, 32603, 29759, 29663

- 3 -

162 (mod 19) = 10, therefore prime 10 is exchanged with prime 1
 29879, 30803, 32183, 32003, 31847, 31607, 31583, 31547, 31259, 31139
 32507, 30539, 30467, 30347, 30323, 30203, 32603, 29759, 29663

536 (mod 19) = 4, therefore prime 4 is exchanged with prime 2
 29879, 30803, 31847, 32003, 32183, 31607, 31583, 31547, 31259, 31139
 32507, 30539, 30467, 30347, 30323, 30203, 32603, 29759, 29663

The primes selected to be used are the first three in the table 29879, 30803 and 31847.

4.3.2 Calculation of P and B values

The Random Session Key generated for this transmission is split into 6 two digit groups. These are modified to increase their size by adding 1024 to each; this ensures that modulation starts as soon as possible. The first three groups are used as the P values, P(0), P(1) and P(2) and the second three are used as the B values, B(0), B(1) and B(2).

4.3.3 Example Calculation of P and B values

Random Session Key = 149162536496

P values:

P(0) = 14 + 1024 = 1038 P(1) = 91 + 1024 = 1115 P(2) = 62 + 1024 = 1086

B values:

B(0) = 53 + 1024 = 1077 B(1) = 64 + 1024 = 1088 B(2) = 96 + 1024 = 1120

4.3.4 Calculation of the Pseudo Random Bit Sequences

The three primes selected as above are used as the moduli for calculations carried out with the Phase and the Base values in the same way as in other uses of the algorithm. Modular arithmetic is carried out using the first P and B values. The first of the three selected primes being used as the modulus.

For example for the first set of prime, P and B:

The P value is multiplied by the B value:

$1038 * 1077 = 1117926$

$1117926 \text{ (mod the first prime)} = 1117926 \text{ (mod 29879)} = 12403$

12403 is then used as the new Phase value and is multiplied by the Base value:

$12403 * 1077 = 13358031$

$13358031 \text{ (mod the first prime)} = 13358031 \text{ (mod 29879)} = 2116$

This process is repeated as often as is necessary to generate tables which are used to encrypt the message. It is also carried out for the remaining two sets of primes, bases and phases. As the calculations are completed the corresponding (mod 2) values of the results are stored in tables X, Y and Z for the duration of the call and are used to encrypt the Main Facsimile Message.

The three tables are of slightly different lengths but the length of each is a prime number. The X table is 1021 elements long, the Y table is 1019 elements long and the Z table is 1013 elements long. The first elements in each table are added (mod 2) to the first bit of the Main Message, the second to the second and so on to the end of the message. When the Main Facsimile Message reaches 1013 bits the Z table is at its end. For the next message bit it starts again at its beginning. When the Y table finishes it restarts and similarly for the X table. As the sequences run out of phase the total message length before repetition of the XYZ is approximately 10^9 bits.

4.3.5 Example of the algorithm generating three separate pseudo random bit streams.

| | | Running Length | | 1021 X | 1019 Y | 1013 Z |
|-------|-------|----------------|-------|-----------|-----------|-----------|
| Prime | 29879 | 30803 | 31847 | | | |
| B(n) | 1077 | 1088 | 1120 | | | |
| P(n) | 1038 | 1115 | 1086 | | | |
| 1 | 12403 | 11803 | 6134 | 1 | 1 | 0 |
| 2 | 2116 | 27616 | 22975 | 0 | 0 | 1 |
| 3 | 10262 | 13283 | 31471 | 0 | 1 | 1 |
| 4 | 18464 | 5297 | 24738 | 0 | 1 | 0 |
| 5 | 7854 | 2975 | 31517 | 0 | 1 | 1 |
| 6 | 3001 | 2485 | 12564 | 1 | 1 | 0 |
| 7 | 5145 | 23819 | 27153 | 1 | 1 | 1 |
| 8 | 13550 | 9749 | 29322 | 0 | 1 | 0 |
| 9 | 12398 | 10680 | 6383 | 0 | 0 | 1 |
| 10 | 26612 | 7109 | 15232 | 0 | 1 | 0 |
| 11 | 7163 | 3039 | 21695 | 1 | 1 | 1 |
| 12 | 5769 | 10511 | 30986 | 1 | 1 | 0 |
| . | . | . | . | . | . | . |
| . | . | . | . | . | . | . |
| . | . | . | . | . | . | . |
| 1011 | 25447 | 28597 | 19176 | 1 | 1 | 0 |
| 1012 | 7376 | 2506 | 12242 | 0 | 0 | 0 |
| 1013 | 26017 | 15864 | 16830 | 1 | 0 | 0 |
| 1014 | 23686 | 10352 | 28023 | 0 | 0 | 1 |
| 1015 | 23035 | 19881 | 18465 | 1 | 1 | 1 |
| 1016 | 9125 | 6822 | 1387 | 1 | 0 | 1 |
| 1017 | 27313 | 29616 | 24784 | 1 | 0 | 0 |
| 1018 | 15165 | 2270 | 19343 | 1 | 0 | 1 |
| 1019 | 16771 | 5520 | 8200 | 1 | 0 | 0 |
| 1020 | 18163 | 29978 | 12064 | 1 | 0 | 0 |
| 1021 | 20685 | 26490 | 8552 | 1 | 0 | 0 |

- 5 -

5. AUTOMATIC MODE AT THE RECEIVER

The receiving machine re-calculates the Mutual Primitive using the Registered Crypt String and is then able to decrypt the Random Session Key using the HKM algorithm as explained in COM 8-D. The Random Session Key is used with the HFX40 algorithm in an identical way to generate and store the same X, Y and Z tables and to use them in the same way as the sending machine to decrypt the Main Facsimile Message.